CONNEXIONS™

The Interoperability Report

April 1989 Volume 3, No. 4

ConneXions—
The Interoperability Report tracks current and emerging standards and technologies within the computer and communications industry.

In this issue:

ConneXions is published by Advanced Computing Environments, 480 San Antonio Road, Suite 100, Mountain View, CA 94040, USA. Phone: 415-941-3399.

ISSN 0894-5926

From the Editor

With this, the 25th issue of *ConneXions*, we begin a new series of tutorial articles on the emerging OSI standards. The series is called *Components of OSI*. In addition to describing all the pieces that make up what we collectively term "OSI," (X.25, FTAM, VT, ASN.1, X.400, X.500, TP, CLNP, Session, Presentation, etc.), the series will also focus on the standards making process, transition and coexistence issues, and other related topics. First out in our new series is a tutorial on the *Integrated Services Digital Networks* (ISDN) by Bob Blackshaw from the Corporation for Open Systems (COS).

The rest of this issue is almost entirely devoted to questions of ethics, etiquette, and computer security. Last November, the Internet was attacked by a computer *worm* (or "virus"). This incident brought to the surface a number of important issues ranging from computer security and reliability to moral and ethical topics. First, John Quarterman of Texas Internet Consulting discusses some guidelines on proper etiquette and ethics for users of computer networks. Peter Neumann of SRI International reflects on the lessons learned from the Internet Worm incident, and finally we include the text of RFC 1087 which states the IAB's position on Ethics and the Internet.

Also included in this issue is another in our series of book reviews, and a letter to the Editor in response to an earlier article.

A reminder about the *Internet Requirements Seminar* which Advanced Computing Environments is hosting in Monterey, California, May 1–2. The seminar will discuss two important documents concerning the implementation of TCP/IP protcols for hosts and gateways: an RFC entitled "Requirements for Internet Hosts," (to be published soon), and RFC 1009 called "Requirements for Internet Gateways." Call us at 415-941-3399 for more information.

For your convinience, we include the dates/locations for the next 6 Internet Engineering Task Force (IETF) meetings below. Contact Karen Bowers at NRI, 703-620-8990 or bowers@sccgate.scc.com for more information.

Date		Location
April 11–14	1989	Kennedy Space Center
July 25-28	1989	Stanford University
Oct 31– Nov 3	1989	University of Hawaii
Feb 6–9	1990	Florida State University (tentative site)
May 1-4	1990	Pittsburgh Supercomputer Center
July 31–Aug 3	1990	University of Washington

Components of OSI: Integrated Services Digital Networks (ISDN)

by Robert E. Blackshaw,
Corporation for Open Systems

Introduction

In order to understand the ISDN concept it is useful to review the history of its birth. Prior to the 1960s, the telephony networks were primarily analog. All of the interworking *Recommendations* of the *International Telegraph and Telephone Consultative Committee* (CCITT) were based upon analog technology. In the 1960s as digital technology emerged, the CCITT realized that to maintain world-wide interconnectability it would be necessary to create Recommendations covering digital transmission systems.

A special study group, Special Study Group D (SSG-D) was formed with the mandate to study *Integrated Digital Networks* (IDN). IDN covered the networks only and there was no idea at that time of extending digital technology to the subscriber loop plant. The user-network interface would remain analog.

ISDN

In the middle 1970s, a paper was submitted to SSG-D proposing that, if the digital technology were to be extended right to the subscriber premises, the IDN could be used to provide all information services. This marked the birth of ISDN and a graceful migration was envisaged from analog, to IDN, to ISDN. However, user demand for innovative telecommunication services overtook IDN and the planned graceful transition will not take place in most countries. At the time SSG-D delivered its final report, the CCITT decided that it would be desirable to have a single study group to oversee ISDN. SSG-D was given permanent status as Study Group XVIII and chose as its prefix for Recommendations the letter **I**.

At first there really was no user demand for ISDN. To quote Dr. Theodor Irmer, Director of the CCITT and former Chairman of Study Group XVIII, from his keynote speech to the ISDN '88 symposium in St. Louis, MO, "Apart from a handful of far-sighted ISDN freaks (not many more than a dozen) who believed in ISDN already at that time (virtually *no* ISDN technology existed in those early days!), a strong skepticism generally prevailed..." This feeling that ISDN was not something that subscribers need prevails to this day in many quarters.

In fact, there is a strong subscriber opinion that all the carriers should be doing is to reduce the cost of existing networks, and stop fooling around with ISDN. The strange part of this is, that these same subscribers are trying to create their own networks, or are complaining that the carriers do not offer the services that they really need. What seems not to be understood by these same subscribers, is that the analog network has reached its maximum development, and that without a fully digital network (from subscriber-to subscriber) further enhancement is not possible.

Thus the now famous *2B+D* interface was developed, operating two 64 kbit/s B-Channels and a single 16 kbit/s D-Channel. The seemingly odd rate of 16 kbit/s for the D-Channel is arrived at as follows: Because clocking at 64 kbit/s or multiples thereof is simpler, the interface operates at three times the basic clock, or 192 kbit/s. The D-Channel rate is simply the amount left after deducting the 48 kbit/s used for overhead and other embedded functions.

Documents

Many aspects of ISDN fall within the purview of other Study Groups and those aspects were sub-contracted to the applicable SGs by SG XVIII. As a result, many ISDN Recommendations bear two numbers; the number of the parent SG, e.g., Q.921, and the number of SG XVIII, e.g., I.441. The decision to give all Recommendations pertaining to ISDN an I.nnn number was simply to have all ISDN Recommendations published in a single fascicle (volume) of the colored book for the convenience of its users. SG XVIII chose the following numbering plan:

I.100 series - General
I.200 series - Services
I.300 series - Network Internals
I.400 series - User-Network Interfaces
I.500 series - Network Interworking
I.600 series - Maintenance

This numbering plan gives instant recognition of a Recommendation's topic simply from its number. This was another reason for double numbering, for without a SG XVIII number, the parent SG's number would be meaningless.

What is ISDN?

Well, just what is this ISDN *thing* that so much is being said, written, and rumored about? Very simply put ISDN began as a digital circuit-switched network. However, thanks to the signalling channel, ISDN is just as capable of providing packet-mode services. Even though ISDN is an all-service network, it is designed to complement the existing telephony and data network and will interconnect with them. ISDN has become a *network architecture* as much as a network system. All of this capability derives from ISDN's new signalling techniques.

Prior to ISDN, when the network was signalled, i.e., provided with the routing information, it was done on the same channel that was later used for information transfer. For example, with a standard telephone set, the handset is lifted and the routing information (subscriber number) is keyed in on the Touch-Tone® pad. As soon as the network switch has determined that sufficient routing information is available to complete the call setup, no further information is accepted—in effect the signalling channel or function is terminated. Apart from the hookswitch the subscriber is unable to signal the network. This analogy applies to almost all networks that signal over the same path that is used for information transfer.

D-Channel

ISDN's separate D-Channel is a full-period signalling channel—*it is always there and always available*. Due to a more complex protocol than pulse or tone signalling, it also provides access to the intelligence inherent in the control functions of modern digital switch machines. The subscriber may have access to as much of this intelligence as the network operator sees fit to allow.

One other aspect of this separate signalling channel concept worth mentioning is the flexibility that it provides the network operators. In the past, in order to provide some distinct new service it was usually necessary to build a complete new network, e.g., packet-switching, etc. However, with ISDN, new services can be introduced simply by making changes to the switch machine software.

continued on next page

Integrated Services Digital Networks *(continued)*

This is not to say that this is a trivial task, but it is certainly much less expensive than a complete new network. From being driven by their engineering departments, the network operators may now be market responsive due to ISDN's inherent flexibility.

Signalling

The concept of a separate signalling channel for the user probably originated in the network operators own use of separate signalling networks, i.e., Signalling System # 6 and Signalling System # 7. The latter system, to be called *Common Channel Signaling 7* (CCS7) in North America, is a vital part of ISDN.

ISDN also incorporates several forms of multiplexing, primarily to derive three (2B+D) channels on a single pair of wires, but has also multiplexed channels at Layer 2. This multiplexing will be discussed later in this article.

The ISDN era should see a portfolio of services offered that is only dependent on the user demand and the regulator's intelligence.

Services

ISDN is described in terms of services that are provided. There are three basic services; Bearer Services, Teleservices, and Supplementary Services. *Bearer Services* are those provided by the three lowest layers, Layers 1-3. *Teleservices* encompass the whole seven OSI layers. *Supplementary Services* are added functionality to the other two services, such things as Call Forwarding, Reverse Charging, etc.

Examples of Teleservices are; Teletex, Videotex, Directory access, etc. ISDN Teleservices are whatever the user subscribes to from the network operator. Teleservices are what the human user sees, be it access to some database, access to a large host mainframe offering several capabilities, or any other overall service.

Teleservices may be internal to the ISDN, and that would be natural as in the case of a database of customer addresses, i.e., a directory. However, the CCITT has not attempted to suggest that such services would only reside within the ISDN, and Teleservices may be provided by third parties.

Examples of Bearer Services are voice circuits, 64 kbit/s clear channels, 3.1 kHz audio channels, etc. The human user's terminal sees the bearer service and with internal software and hardware, uses it to provide the overall teleservice to the human user.

Any of these two prime services (Teleservice and Bearer Service) may be enhanced through the provision of various Supplementary Services so that they perform more than the basic functions.

Wiring

Premises wiring may be done in several ways. The simplest is the point-to-point wiring scheme where only a single terminal device is supported.

The wiring scenario expected to be most popular is the *short passive bus*. This could represent a multi-jack residence or a single employee's work center. Provision is made to take up to 8 devices.

The passive bus also comes in an *extended* format, typically for Private Automatic Branch eXchange (PABX) environments where there would be a long loop between the work center and the PABX.

The length is in the order of 1 km with all of the terminal devices clustered in the last 25-50 meters. The number of terminal devices is left to the network operator to stipulate. At a recent meeting of SG XVIII a new wiring scenario was adopted known as a star *NT1*. In this scenario, more than eight devices may be wired in a star fashion.

Protocols

ISDN does not specify any new protocols for the B-Channels above Layer 1. If the user wants a clear 64 kbit/s channel, he selects the appropriate protocols. Similarly, voice and packet-mode has to be selected by the user. The new ISDN protocols mostly apply to the D-Channel. The signalling protocols are:

I.430 and I.431 for Layer 1 (applies to all channels)
I.440 and I.441 for Layer 2 (LAP-D)
I.450 and I.451 for Layer 3 (Entity S)

Layer 1

Layer 1 has two separate protocols for either side of the NT1 (loop termination) device, one for the user side and one for loop side. Each will be discussed in turn, beginning with the user side of NT1.

User side

The user side of NT1 protocol is defined in Recommendation I.430 for the Basic Rate Interface. This interface supports two B-Channels at a 64 kbit/s rate and one D-Channel at a 16 kbit/s rate.

ISDN has a very unique first layer. It employs some interesting forms of multiplexing, not only to separate the two B-Channels and the D-Channel, but also to allocate the D-Channel among the eight terminals on the passive bus.

Multiplexing of the two B-Channels and the D-Channel is done using a straight Time Division Multiplexing scheme. In each Layer 1 frame there are 16 bits for each B-Channel and four bits for the D-Channel.

Since the passive bus scenarios allow up to eight terminals per loop, there is another level of multiplexing on the D-Channel that ensures equal access to the D-Channel by all terminals. It is somewhat like a Carrier Sense Multiple Access (CSMA) except that it is data that is sensed rather than carrier. What makes it unique is that it has Collision Resolution rather than mere Collision Detection. It could be called *Data Sense Multiple Access/Collision Resolution* (DSMA/CR). Of course, such a scheme requires a fairly complex protocol and this is where 16 kbit/s of the 48 kbit/s of overhead is consumed, the other 32 kbit/s are taken up by echoed D-channel bits, DC-balancing, framing and synchronization, etc. (2 x 64 + 16 = 144 and 192 kbit/s - 144 kbit/s leaves 48 kbit/s of overhead).

In operation on the passive bus, all terminal devices are provided with an echo of the bits received by the NT device on the D-Channel. Each terminal device examines this echo for contiguous binary one bits. If eight one bits are counted, the channel is assumed to be idle and the terminal device may begin sending a single Layer 2 frame. It continues monitoring the echoed bits to ensure that the NT is receiving exactly what the terminal is sending. Any discrepancy (a collision) causes the terminal to cease transmitting. Due to the characteristics of the protocol, one terminal will see no discrepancy and so wins (resolution) the channel and continues transmitting.

continued on next page

Integrated Services Digital Networks *(continued)*

Loop side

After all of the unique things on the subscriber side of NT1, the loop side is rather prosaic. It is point-to-point (no contention here), and needs only transmit 144 kbit/s of user information. Typical overhead is in the order of 16 kbit/s giving a loop data rate of 160 kbit/s. However, 160 kbit/s on 22, 24 or 26 gage telephone cable is quite tricky for cable plant that was designed for 4 kHz analog voice use.

Various schemes were proposed for this U interface, mandated by the FCC. The final choice was to use the Echo-cancelling technique, with *Decision Feedback Equalization* (DFE), and to use a 2B1Q (2 Binary 1 Quaternary) line code.

A 2B1Q line code simply means that every line symbol conveys two binary bits of information. Given that two binary bits may have four states, a quaternary or four element line code is necessary. This has an advantage in that it reduces the line rate to 80 kbaud, thus improving the loop distance that may be covered.

Echo-cancelling is a technique that enables full-duplex transmission on a single pair of wires. Laboratory tests indicate that this technique will cover 99% of the standard loops in the U.S. The standard loop is defined as 18 kilofeet. In actual practice some areas have longer loops than this and some form of remote concentration will be needed for such areas.

Most of this technology is currently available in the form of Large Scale Integrated (LSI) silicon. The loop technique was recently sent to vote in T1, the ANSI telecommunications sub-committee.

Layer 2

ISDN, as stated earlier, uses the *HDLC* ISO standard at Layer 2. In this CCITT implementation it is referred to as *Link Access Procedure-D* (LAP-D). It is a standard sub-set of the HDLC protocol and follows all of HDLC's conventions.

LAP-D uses the Balanced mode configuration of HDLC where both stations are equal, referred to in HDLC documents as a Combined Station. The set of commands used are;

Information (frames)
Receiver Ready (RR)*
Receiver Not Ready (RNR)*
Set Asynchronous Balanced Mode Extended
Disconnect (DISC)
Reject (REJ)*
Unnumbered Information (UI)*
Exchange Identification (XID)*

The commands marked with the asterisk are also used as responses and the following responses are also used;

Unnumbered Acknowledge (UA)
Disconnected Mode (DM)
Frame Reject (FRMR)

LAP-D differs from earlier implementations of HDLC in that it uses a two octet address space. The HDLC standard permits multi-octet addressing, however, until LAP-D the single octet address has been the norm.

SAPI and TEI

ISDN uses this two octet address to accomplish two forms of multiplexing on the D-Channel. A six-bit address space is used as a *Service Access Point Identifier* (SAPI) to multiplex a single terminal's D-Channel between various service functions (Signalling, Packet, Telemetry, Management, etc.) The second portion of the address, a seven-bit *Terminal Endpoint Identifier* (TEI) allows multiplexing of a number of logical D-Channels onto the single physical D-Channel. Note that the short passive bus limitation of eight terminals applies to physical devices, each physical terminal could contain multiple logical terminals.

SAPIs are assigned to specific services so that ISDN's functions may be accessed in a specific manner;

0 = Signalling
1 = New Packet Mode Services
16 = Packet Mode Access
63 = Management

Signalling is the priority function of the D-Channel, but equally important is the Management function. It is this function that assigns and removes Terminal Endpoint Identifiers. TEIs come in two flavors, fixed and dynamic. In the total range of 128 TEIs, 0 to 63 are for fixed assignment, 64 to 126 are for dynamic assignment, and 127 is reserved for broadcast use.

A terminal with a fixed TEI usually has it wired in or set by means of a switch. Terminals with dynamic TEIs negotiate with the Management function for an available TEI. This negotiation is done with the UI command/response without the need to establish the LAP-D link. This is for terminal portability purposes. For example, if a user has a portable computer connected to an ISDN PABX at his/her office with a TEI of 102 and decides to take the portable home, he could find that some device in the home already uses TEI 102.

With dynamic assignment this is no problem because a new TEI can be negotiated with the network. Terminal portability is a strong point of ISDN and one more reason for adhering to a world-wide standard. Layer 2 was originally designed to use modulo 8 and modulo 128 operation, but in 1986 the modulo 8 option was dropped. In fact, the latest versions of I.440 and I.441 have removed all options but one.

The sole remaining option concerns the use of the XID frame and is fairly simple to resolve. The basic use of XID is to negotiate non-default values of certain Layer 2 timers and retransmission counts with the network.

The Terminal Endpoint (TE) sends an XID frame containing the proposed new values in the information field to the network. If the network allows such negotiation, it responds with its proposed values. This is a one-shot operation, whatever the network proposes is its final offer and no more negotiation takes place. If, however, the network does not allow negotiation, it simply responds with an XID frame that does not contain an information field. In this case the TE knows that the default values apply.

continued on next page

Integrated Services Digital Networks *(continued)*

ISDN's LAP-D is a true sub-set of ISO's HDLC and follows all of the rules of HDLC. This is a proven and robust standard, so there is little likelihood that Layer 2 will pose any problems. In addition, use of HDLC with its bit-stuffing technique is vital to Layer 1, else the contention resolution scheme would not work (bit stuffing makes it impossible to have more than five 1 bits in a contiguous data sequence, and as you will recall, the contention resolution seeks a contiguous eight bit sequence). This may be a slight violation of the OSI Reference Model, but it is unlikely that any modern system would have chosen a character oriented protocol for Layer 2, so the discussion is moot.

Layer 3

ISDN uses a message (packet) oriented protocol at Layer 3 that serves as a negotiation protocol as well as a signalling protocol. It is the user's methodology for not only requesting a connection, but also for defining the parameters of that connection. It is comparable to having the line marketing function of the network operator built into the network. Currently, ISDN will support the following connection types:

Voice
Alternate voice - data
3.1 kHz audio (for modems)
64 kbit/s non-restricted
64 kbit/s restricted
384 kbit/s (H0 rate)
1.536 Mbit/s (H11 rate)
X.25 Packet-Mode (on B or D channels)

Other modes are proposed, such as 7 kHz audio, 15 kHz audio, broadband (32 Mbit/s and up), and new forms of packet mode services based on use of LAP-D currently known as Frame-Relaying and Frame-Switching.

The I.451 protocol messages are sub-divided into four groups:

Call Establishment Messages
Call Information Phase Messages
Call Clearing Messages
Miscellaneous Messages

The basic I.451 protocol header consists of four or five octets, depending upon the terminal type. The first octet is a Protocol Discriminator, thus allowing other protocols (X.25 packet level) to operate on the D-Channel. A seven bit message identifier allows up to 128 message types.

In each message there is a *Call Reference* value, a randomly generated number that is used to distinguish call messages on a given interface. For example, on a basic interface the TE could be attempting call setup on both B-Channels simultaneously and the Call Reference is the only means of distinguishing messages. This field is one or two octets depending upon the interface type and operation.

Finally, the various information elements are attached to the header. The information elements themselves cover a seemingly endless set of parameters that are used to establish the nature of the connection being setup or requested. Things such as which B-Channel is to be used, whether it is voice, data, audio, or video, and the calling and called party numbers and addresses are included. Whether rate adaptation is being used, and if so what rate was adapted is also specified. The header also includes information on which lower and higher layer protocols that are being used. Choice of transit network(s) is allowed. In short, just about every detail imaginable about the connection is provided in the header.

The ISDN signalling protocol is powerful and certainly has ample room for the foreseeable future. It has turned out to be more complex than originally thought and will not be the simplest thing to implement, but will no doubt someday turn up on a piece of silicon.

Other uses

Although the D-Channel was originally designed for signalling purposes only, the realization that the 16 kbit/s bandwidth was more than ample for setting up and tearing down only two B-Channels led to other uses.

One of these uses is the operation of X.25 packet mode terminals on the D-Channel at medium data rates. This is one of the options of adapting packet-mode terminals.

The third and final operational mode of the D-Channel is for telemetry. This is envisaged as operation with an average bit rate of 50 bit/s or so (although any device on the D-Channel is clocked at 16 kbit/s). Since telemetry is primarily a national service no protocols have been designed for its use. Telemetry covers such functions as remote meter reading, building alarms, etc.

It may well be that telemetry is an area that could see the greatest innovation with ISDN. Depending upon the regulatory climate, it may be the biggest money maker for ISDN, both providers and users.

Adaption

The CCITT did not forget that there are large numbers of existing terminals that must somehow be accommodated. This is the role of the *Terminal Adaptor* (TA). The existing terminals (TE2s) are supported by the TA function and together, both units could be considered as a TE1 (ISDN terminal).

There are several techniques provided for universal adaptation schemes for V.-series, X.21, and X.25 terminal devices. These schemes are not exactly efficient in their use of bandwidth but do offer a type of "open system" approach. As regards efficiency, it should be remembered that using a 4800 bit/s modem on a voice (64 kbit/s) circuit is not efficient either. Cost is the governing factor.

The Recommendations written for rate adaptation have only dealt with the existing bit rates based on the multiples of 75 bit/s. At first only synchronous devices were to be accommodated but now asynchronous devices are supported as well. Rates from 75 bit/s to 56 kbit/s can be used.

continued on next page

Integrated Services Digital Networks *(continued)*

This function should be called Rate + Function Adaptation to be correct, since not only are the data bit rates adapted, but also the modem control leads of the existing interface, i.e., the status of such signals as *Clear to Send* (CTS), *Ready to Send* (RTS), etc. are conveyed in the frame structure of the adaptation technique.

Rate adaptation involves converting the old rate to the nearest 8 kbit/s sub-multiple of the 64 kbit/s B-Channel rate. Because of the function adaptation certain rates less than 8, 16, or 32 kbit/s must actually be increased to the next sub-multiple, e.g., 7200 bit/s must be increased to 16 kbit/s.

In addition to the rate adaptation function, a TA may also multiplex several rate adapted streams onto a single 64 kbit/s B-Channel. For example, if there were 8 TE2 units attached to a single TA, each operating at an adapted rate of 8 kbit/s, all eight TE2s could be multiplexed onto one B-Channel. Of course, because the ISDN switches 64 kbit/s channels, all eight TE2s would be connected to the same called ISDN number.

During the last CCITT Study Period, a technique of using the LAP-D framing structure and an asynchronous time division multiplexing technique for rate adaptation was approved. This was referred to as Recommendation V.tad during its creation, but has now been assigned the number V.120.

The various Recommendations are designed to provide a *universal* technique for interoperability. For private networks operating over ISDN there is nothing to prevent users from simply attaching a digital multiplexor to either end of the 64 kbit/s channel and using whatever method it provides. There is also no particular reason why any terminal device that is accustomed to deriving its clocking from the DCE could not clock at 8 kbit/s rather than 4.8 kbit/s, or 16 kbit/s rather than 9.6 or 14.4 kbit/s.

Primary rate

This article has dealt mainly with the Basic Interface, the 2B+D. The other interfaces, two flavors of Primary Rate, provide more channels (23B+D for North America and Japan and 30B+D for the rest of the world).

The difference is caused by the fact that there are two DS1 rates in use (DS1 is the reference number of the first multiplexing stage in the digital hierarchy), North America and Japan (the so-called μ-law countries) use a DS1 rate of 1.544 Mbit/s. The rest of the world (the so-called A-law countries) use a DS1 rate of 2.048 Mbit/s.

The Primary Rate interface of interest here is the 23B+D - 1.544 Mbit/s case. The U.S. draft standard is based on the existing T1 carrier *Extended Superframe Format* (ESF). The basic T1 format is a 193 bit frame consisting of a single framing bit and 192 information bits divided into 24 octets providing 24 64 kbit/s channels (in the Primary Rate interface the D-Channel operates at 64 kbit/s).

The ESF format connects 24 of these 193 bit frames into a superframe and uses some of the framing bits for a CRC check as well as an embedded operations channel. Note that there will not be any A and B signalling bits in the ISDN format.

Planning

ISDN promises a new and more flexible network service to users. Despite all of the commentary in the press, it will find users. There are several enhancements to the user-network interface being studied for broadband service, one at 45 Mbit/s and another at approximately 150 Mbit/s.

Service enhancements include several Supplementary Services, sorely lacking in the CCITT *Red Book* version. Other planned service enhancements are the two Frame Modes, a packet-mode type of service using LAP-D and a null Layer 3 protocol. There is also a high speed Broadband interface planned.

Frame Relaying operates end-to-end, i.e., the network does not intercept Layer 2. This mode would propagate CRC errors end-to-end even if they occur at an early node-to-node hop in the connection.

Frame Switching intercepts Layer 2 at each network node and would intercept and request retransmission of packets with CRC errors.

The Frame Mode services are possible because ISDN has pushed the multiplexing functions down one layer as compared to X.25 Packet Mode.

Broadband ISDN (B-ISDN) proposes three new information rates;

H21 @ 32768 kbit/s
H22 in the range of 43 to 45 Mbit/s
H4 in the range of 132 to 138 Mbit/s

B-ISDN will use a form of asynchronous time division multiplexing called Asynchronous Transfer Mode (ATM), which promises to provide a type of bandwidth on demand service. Only initial descriptions are in the new CCITT *Blue Book*.

Summary

ISDN is not simply a digital network, offering two or more channels on a single loop, as stated earlier—*ISDN is an architecture*. Where the real value of ISDN lies is in the flexibility it offers to the network operators in providing new services at more reasonable costs. It also offers new potential to users in the access provided by the D-Channel to the intelligence inherent in any modern digital switch. There will be services and features offered that no one of us even imagines at this time, and that is perhaps the real advantage of ISDN—it is really only limited by our imagination and intellect.

ROBERT E. BLACKSHAW is an Assistant Manager—Strategy Forum Support at the Corporation for Open Systems, International in McLean, VA. He has spent 38 years in the communications field, beginning with Bell Canada in 1950. He worked in many departments, Plant, Engineering, and EDP. He was involved in the planning of DATApac® and finally retired in 1983 from Network Systems Group's long range planning. He worked briefly with Omnicom, Inc., a VA based consulting and educational company. He joined COS in 1987 where he is involved with subcommittee support and mainly with ISDN. He has been an active participant in the standards arena since 1975

Etiquette and Ethics

by John S. Quarterman,
Texas Internet Consulting

Introduction

Learning how to use a computer system properly takes much longer than simply learning the mechanics of making it do things [1]. Learning to use a system without offending other users and to maximum benefit involves *etiquette*. Learning to use a system without causing harm to others involves *ethics*. These are not completely separable subjects, and the former tends to blend into the latter as the seriousness of the situation increases. This article presents a discussion of these subjects, and some suggested guidelines for appropriate behavior. It is an extract from a forthcoming book, *The Matrix: Computer Networks and Conferencing Systems Worldwide*, to be published by Digital Press. Perhaps its publication here will spark discussion.

Sources

This article draws on several documents, including an early Rand report on ethics and etiquette for electronic mail [2], guidelines posted monthly on USENET for several years [3,4], other guidelines developed from the experience of a more exclusive small group [5], and some resolutions on ethics adopted by BITNET and CSNET [6] and NSFNET [7] after a recent (November 1988) and very publicized problem on the Internet. The guidelines presented here were chosen as being common to several of these documents, guided by personal experience. Problems of etiquette are often associated with *Computer Mediated Communication* (CMC), (services like mail and conferencing), while ethical problems seem to often have to do with *resource sharing*, (services like remote login and file transfer). However neither kind of problem is limited to any single kind of service.

Etiquette

Problems of misunderstanding and rudeness are matters of *etiquette*. One of the most obvious effects of networks is a tendency of users to *flame*, that is, to produce many words on an uninteresting topic, or in an abusive or ridiculous manner; "raving" is almost a synonym for flaming. The usual supposition for why computer networks tend to aggravate flaming is that the flamer is isolated from the readers and has no negative feedback to reduce this behavior. No immediate feedback, perhaps, but flamers tend to get many mail replies (this kind of attention may actually be what some of them want). Here are a few guidelines for etiquette:

- *CMC Services Are Not Like Other Media:* CMC media are not like other media, no matter how many superficial similarities there may be. Treating a CMC service just like the telephone, paper mail, or any other medium, will lead to misunderstandings and mistakes. Even if you are using CMC to communicate with people you know well, you won't see them the same way with CMC services.

- *Emulate Experienced Users:* The best way to learn is by emulating others who have already learned how to make best use of a system, with etiquette, and ethically.

- *It's Not Just a Machine:* All that is in front of you may be a piece of hardware, but there are people on the other end of CMC services, and there are people responsible for maintaining and developing resource sharing services.

- *Be Brief:* Using many words is more likely to cause misunderstandings than using a few well-chosen words. People are also less likely to read long messages: more than a page or two is probably too much. When responding to a message and including part of it for context, include as little as possible while maintaining clarity and precision.

- *Label Your Message:* Choose a title that fits the subject and stick to it. If you need to bring in another subject, consider posting an additional message. Supply keywords if the system supports them.

- *Remember Your Audience:* When sending a message, remember who will be reading it, and tailor it to them. Use language, references, and subjects that will be comprehensible. Don't use buzzwords or other terms the audience won't know, unless you define them. Be aware that certain topics are objectionable to some people.

- *Choose an Appropriate Medium and Forum:* Use a conference or mailing list on a topic related to that of your message. Don't crosspost to many different fora without thinking about which ones. Use a style appropriate to all of the topic, the medium, and the forum (e.g., a chatty conversational style may be appropriate for a social conference, but not for a serious technical discussion group). Sometimes personal mail is most appropriate for clarifications or criticisms. Other services may also be appropriate, as has been discussed at length above. Be aware that some systems prohibit certain types of messages, such as commercial advertising. Don't try to duplicate traditional news media: assume everyone will have heard of a natural disaster or political assassination, and that you don't have to tell them the basic outline.

- *Identify Yourself:* Sign your message with some appropriate information such as your name and your affiliation. If you have several affiliations (work, hobby, professional association), pick one appropriate to the subject. Sometimes anonymity is appropriate. In general, choose and make plain an appropriate *identity*. But don't use lengthy signatures with long quotations or large graphics; they waste resources and annoy people.

- *Observe Technical Restrictions:* Much computer software and display equipment cannot handle lines longer than 80 characters. Escape sequences that cause one effect on one device may do something entirely different on another: don't use them unless you're sure they're standard. Control characters in general may have varying effects, and are often not passed through intervening links: avoid them (even tab characters) when possible.

- *Avoid Formatting Problems:* Adjusted right margins are hard to read without proportional fonts. Lots of vertical white space just takes up space. Paragraph breaks are very useful.

- *Post New Ideas:* If you have something to say and noone else has said it, do so. But try not to just repeat what has already been said, except in brief confirmation.

continued on next page

Etiquette and Ethics *(continued)*

- *Respond to the Topic, Not the Person:* Avoid ad hominem attacks, and try to understand what the person is saying. If you can't tell from what they wrote, ask. If you must criticize someone, attempt to give them a chance to respond. If you comment on the style of a message, respond to the content as well.

- *Read Other Messages Before Responding:* Don't dash off a message making an obvious response: somebody else has probably already made the same response. Read all the relevant message first to see if you're the first.

- *Don't Respond in Anger*: Wait a few minutes or hours, or even until the next day. Anger feeds on anger, especially in CMC media, where body language and tone of voice are not present. Read any later messages. Consider asking for clarification. If you are still angry when you respond, say so.

- *Give the Benefit of the Doubt:* Mistakes, misunderstandings, and ignorance are far more common than maliciousness. Don't take offense without evidence.

- *Be Careful with Humor and Sarcasm:* Many people have trouble recognizing these things even in person. With CMC, it's best to label them somehow or to avoid them altogether. There are typographic conventions which have developed on the various networks to get around the difficulties of expressing subtleties of expression through ASCII characters. One of the more universal is that UPPER CASE means shouting (much to the chagrin of those with microcomputers that only have upper case). Some *surround phrases with asterisks* to indicate emphasis, while others s p a c e the characters out. People will mark sarcasm <sarcasm> or irony <irony> by stage instructions in angle brackets. Facial expressions often get similarly spelled out: <grin>. There are many ways to indicate the start of a flame, such as FLAME ON! There are shorter ways to indicate lack of serious intent: :-) (Look at it sideways, you'll see why it's called a *smiley face*.) As users become more sophisticated, some eschew these lexical aids in favor of more evocative writing.

- *Be Encouraging and Polite:* New (and old) users tend to be hesitant. The most effective encouragement is often a simple response acknowledging a posting.

- *Discourage When Necessary:* But do it privately and politely. Use personal mail if you can, and public conferences only when necessary. Don't discourage at all unless you're sure it's needed and that you are an appropriate one to do it.

- *Assume Permanence and Ubiquity:* Anything you post to any CMC medium or release through any resource sharing service may be saved permanently, with or without your knowledge, and may be read by anyone at all, any time at all, anywhere at all. Readers may include anyone from national security agencies, to your boss, to your employees, to your family, to the print or broadcast media. Many conferencing systems support privacy features, but they probably keep backups, too.

Ethics Destruction of data or property, disruption of facilities depended upon by others, loss of time, physical harm, and loss of life, are problems of *ethics*. Some simple examples of ethical problems are viruses and worms.

Viruses A *virus* is a program that infects a computer system by inserting itself into another program, replicates itself, and manages to infect other computers by being carried along with the infected program. Viruses in personal computer programs have been a serious problem for several years.

Worms A *worm* is a program that uses network communication facilities to transport itself from one computer on a network to another, and then to repeat the process. Unlike a virus, a worm does not usually insert itself into other programs, nor is it usually passed along by being carried inside another program. There was a very well-publicized worm in the Internet in November 1988. It replicated itself so quickly that it overloaded many of the machines it reached, apparently having escaped from its creator before it was finished.

Both worms and viruses are often constructed as games or to make political points by people who mean no harm, and many of them do not actually cause any direct damage. But even an apparently harmless virus or worm can take large amounts of time on the parts of many people in order to determine that it is harmless.

Ethical guidelines are more difficult than ones for etiquette, but a few plausible ones are given here.

- *Observe Copyrights:* Don't quote text verbatim if it is copyrighted or covered by a restrictive license. Unless you have a philosophical objection to intellectual property, remember that breaking a copyright or licence probably takes income away from the owner.

- *Cite Sources:* When presenting an idea that originated with someone else, give proper credit, whether by naming the source or by citing a formal bibliographical reference.

- *Be Careful with Private Correspondence:* Do not redistribute private correspondence without permission. Don't read other people's mail without permission. If you receive a message by accident, return it to the sender or forward it to the intended recipient.

- *Be Honest:* Don't distribute false information, and don't pretend to be someone you aren't in order to take unfair advantage of someone else.

- *Remember Someone is Paying the Bills:* Even if you are paying to send a message, other people are also having to pay to read what you post. If you are not paying, somebody is, whether it is the system operators, message recipients, or the taxpayers. Stick to useful information distributed to appropriate people.

- *Don't Post Harmful Instructions or Information:* Posting credit card numbers will probably cost someone else. Posting recipes for bombs may result in physical harm.

continued on next page

Etiquette and Ethics *(continued)*

- *Resource Sharing Services are Not Like Anything Else:* A computer network is not like a home computer, or any other single computer. The damage that can be caused by mistakes or malevolence increases with the power and extent of the system.

- *People Depend on Networks and Conferencing Systems:* Damaging such a system damages people.

- *Leaving a Security Hole Unfixed Invites Abuse:* A system administrator who installs a system with a well-known user and password combination or fails to fix a network service security problem to which the solution is well-known invites abuse. Vendors who distribute systems with such problems contribute to the problem, and increase the likelihood of widespread abuse. Users who choose obvious passwords should know they are increasing the risk of damage not only to their own files but to those of others.

- *Using Security Holes to Cause Damage is Wrong:* Regardless of the origin or notoriety of a security hole, using it to cause damage is wrong.

Most of these guidelines are merely common sense and will be readily recognizeable to the reader. They are set forth here as a reminder and because such rules of conduct are seldom gathered together in one place. It is particularly useful to consider these issues in light of the recent problems in the Internet. Perhaps remembering these guidelines can prevent future problems.

References

[1] Turoff, M., "Management Issues in Human Communication Via Computer," in Emerging Office Systems, pp. 233-257, Ablex Publishing Corporation, 1980.

[2] Shapiro, N.Z., & Anderson, R.H., "Toward an Ethics and Etiquette for Electronic Mail," Rand Corporation, 1985.

[3] Von Rospach, C. & Spafford, E. "A Primer on How to Work With the USENET Community," news.announce.newusers, 1988.

[4] Spafford, E. & Horton, M., "Rules for posting to USENET," news.announce.newusers, 1988.

[5] Umpleby, S., "General Systems Theorists' Online Group Process Guidelines," ENA NETWEAVER, Vol. 2, No. 9, 1986.

[6] "Joint Ethics Committee," BITNET & CSNET, 1988.

[7] DNCRI-DAP, Ethical Network Use Statement, Division Advisory Panel, Division of Networking and Communications Research and Infrastructure, National Science Foundation, 1988.

JOHN S. QUARTERMAN received an A.B. from Harvard College in 1977. He worked on networking projects for BBN from 1977 through 1980, and then for the University of Texas. He is a partner in Texas Internet Consulting, who design and install Local Area Networks, and are involved in UNIX standards and programming. He is a member of the Board of Directors of USENIX and has been involved in their networking experiments, such as UUNET.

Book Review

An Introduction to TCP/IP by John Davidson, ISBN 0-387-96651-X or ISBN 3-540-96651-X, published by Springer-Verlag, 1988. This is a short (100 pages), but rather nicely written and laid-out book. It is properly titled an *introduction* and has a brief but accurate historical summary of the evolution of the TCP/IP protocols from their origin in the Arpanet project.

The book is an interesting mix of the abstract and specific. Occasionally, detailed views of the bit layout of headers are shown, but, for the most part, the protocol descriptions are kept to concept level.

I have only a few nits to pick:

- The MILNET is characterized as a military research net but actually it is essentially an operational facility (page 2).

- A list of DARPA sponsored research sites is offered on page 3 which may lead the reader to think the sites mentioned are the only members of the Internet community. Even the early community included many more sites.

- On page 5, INWG is called the Internet Working Group. Actually, it was the *International Network Working Group* and was the forerunner to IFIP 6.1 (I know, I was the first chairman of INWG and moved it under IFIP support in 1974).

- On page 94 there is a wonderful typo in the title of a reference paper: "A Protocol for Pocket Network Interconnection."

My biggest complaint, however, is the handling of the IP protocol. The author tries very hard to find a way to put IP at layer 3 (network layer) of the OSI model. This is fine, but to do this, he insists on placing networks such as Arpanet at layer 2 (link layer). This is simply *wrong*. The OSI network layer comprises an upper and lower part. The upper part is the Internet sublayer and the lower part is what the TCP/IP suite calls the Network layer and properly represents the interfaces and functions of networks such as Arpanet X.25 nets and so on.

The book's text is skewed by this struggle to somehow make networks lie at the link layer. The actual descriptions of network function are satisfactory—they just look and sound odd when characterized as link level functions.

The other omission in figures illustrating the Internet (such as Fig. 1-1 and 1-2) is the absence of explicit routers/gateways between the networks. The concept of encapsulating IP packets in lower level network layers is an important one which should not be ignored. It is that concept which permits packet networks of different types to intercommunicate by way of the IP protocol.

On the whole, however, the book offers a very useful summary which conveys the concepts and general scheme of the internet technology, which was its intent.

—Vint Cerf

Long-Term Implications of the Internet Worm

by Peter G. Neumann, Computer Science Laboratory,
SRI International

Introduction

The "Internet Worm" of early November 1988 involved remote penetrations of thousands of Berkeley-UNIX-based systems on the Arpanet and MILNET. Several vulnerabilities in those systems were exploited by the worm, including trapdoors in the implementation of the electronic mail protocol (*sendmail*) and the user-status query (*finger*). For detailed examinations of the worm software and its effects, see the cited reports by Eichin and Rochlis [88], Seeley [88], and Spafford [88].

The Internet Worm appears to have been an extremely misguided experiment by a graduate student. Although its intent may have been to cause no discernible effects, its actual effects were highly disruptive, causing many computer users and administrators considerable grief when their systems ground to a halt or were shut down for defensive purposes. The disruptions appear to have resulted from programming errors in the worm itself. But the effects could also have been much worse. Sensitive information could have been copied. Trojan horses could have been planted, e.g., containing time bombs. Files could have been subtly altered. Mass deletions could have taken place—although systems with proper backup would have been able to recover from that. It is important to realize that such risks exist widely.

In any event, the Internet Worm must be considered as a highly antisocial act. Most analyses to date have considered its mechanics. We focus here instead on the long-term consequences, i.e., the more global implications that can be drawn from it.

Worms vs viruses

There has been much heated debate about whether the Internet Worm penetrations constituted a *worm* or a *virus*. It penetrated a variety of systems, and propagated itself further. Its intent was worm-like (in the sense of Shoch & Hupp [82]). It did not attach itself to other programs, and therefore was not strictly speaking a virus. It certainly had contaminative properties; whether they were bacterial or virus-like or even retro-virus-like is more or less irrelevant.

Terminology is often perverted. Many of the personal computer "viruses" are really Trojan horses. Many other so-called viruses are simply trap-door or penetration problems. What is most important is the security problem in general.

Computer security and non-security

One of the most important conclusions is that many of our computer systems and networks are fundamentally flawed when it comes to security. UNIX systems (and particularly the Berkeley variants that were victimized) are very popular, representing something like half of the computer systems used in the Internet (but only 20% of those on MILNET). However, UNIX systems are not the only ones with serious vulnerabilities. Many other popular computer systems are intrinsically flawed and vulnerable to intentional misuse by both authorized and unauthorized users. Furthermore some of these systems are used in applications that are themselves realistically subject to penetration attacks and internal subversions. The existing flaws permit many vulnerabilities such as unintended reading and modification of files, loss of system integrity as well as program and data integrity, denials of service, subversion of the application, etc.

The Arpanet vs The Real World

The Arpanet is a *research* environment. Thus it and its host systems have existed within a somewhat cavalier attitude toward security. It is widely believed that promulgation of ethics and peer pressures should be enough to maintain adequate security and integrity. However, one of the grave dangers is that the Arpanet technologies have been used or have influenced applications that are much more sensitive to hostile attacks. For example, MILNET uses the identical technology, but contains systems that might be considered sensitive but unclassified.

Computer systems often do not perform the way they are expected to (especially when stressed), even in the presence of completely benevolent people. Thus, it is very dangerous to create a situation in which system behavior must depend on proper human behavior as well as sufficiently flawless design and implementation. The fallibility of both computers and people must be a fundamental concern, particularly in life-threatening or life-protecting applications.

Ethics, laws, and Good Behavior

It is easy to say that attacks on computer systems are immoral, unethical, and perhaps even illegal. But that will not stop the truly malicious attacker, whether motivated by espionage, sabotage, greed, or whatever. The Chaos Computer Club attacks and the Wily Hacker (Stoll [88]) are ample illustrations.

Certainly there is a need for better teaching and greater observance of ethics, to discourage computer misuse. However, we must not configure computer systems in critical applications (whether proprietary or government "sensitive but unclassified," life-critical, financially critical, or whatever) if those systems have fundamental vulnerabilities. In critical applications, we should never assume the presence of a perfectly behaved community that consists only of legitimate users with no malevolence; thus ethics and good practices address only a part of the problem.

Tradeoffs

There are of course many tradeoffs. A free society suggests that data and program access should be relatively unrestricted, but proprietary and privacy needs are also vital. Ease of modification is desirable, but must be tempered with assurances that there has been no tampering or accidental changes—including the introduction of accidental errors, Trojan horses, etc. In general, programs are easy to write but good programs are very hard to write. Thus, there is a need for better operating systems, networks, system/network interfaces, sounder programming languages, and better software development tools. There is also a need for a much greater awareness of the problems and potential solutions.

Responsibility must of necessity be widely distributed. We certainly need better ethics and better laws, and better teaching of their implications. We also need a society that respects them. But our society needs much more that that; those of us who look at the world only from the vantage point of our computers are missing much.

Deeper problems

Unfortunately, reality suggests that even the best ethics and laws will be violated by people responding to misplaced incentives (financial or otherwise). (The drug situation and insider trading are two examples that are difficult to combat with ethics and laws alone. They are deep social problems. And hacking can certainly become a social disease!)

continued on next page

Implications of the Internet Worm *(continued)*

Thus, we also need computer systems that can enforce security and integrity much more thoroughly, and we need those systems to be administered and used intelligently. But by now it is generally realized that we cannot depend only on computer security controls—there are just too many ways to break them in most systems. Furthermore, by extension, we also cannot depend on computer systems to solve problems that must rely on human judgment, honesty, and good will.

Vendors' responsibilities

UNIX was never intended to be used in highly competitive environments—it was created as a highly flexible system for computing among more or less equally trusted colleagues. Because of its many virtues, it is increasingly being used in more critical applications. It is clear that the system vendors must take responsibility for developing better systems and networks. It is encouraging that several efforts are well underway to produce UNIX variants that support mandatory security (e.g., multilevel security with compartments). These systems will be significantly more secure than vanilla UNIX systems. They will also be subjected to much greater scrutiny and configuration control. Arguments that mandatory security is irrelevant in nonmilitary applications are nicely dispelled by Steve Lipner's 1982 paper. I believe that mandatory security and some sort of mandatory integrity controls will be widespread in a few years.

It is important to note that even the most secure systems can be compromised by improper networking. For example, the use of local and global networks with unencrypted data means that authentication sequences (passwords, tokens, etc.) are transmitted in the clear and can easily be compromised. The authentication problems are difficult, and must not be underestimated.

Conclusions

The computer security vulnerabilities are pervasive in most existing computer systems. Even the best systems can be compromised by improper networking. Even the best networks of secure computer systems can be compromised by improper use and administration. The Internet Worm serves to remind us that considerable care must be devoted to all aspects of the security problem—better systems, better networks, better teaching of ethics and social responsibility, and better understanding of the vulnerabilities, risks, and intrinsic limitations. Perfect security is impossible. If the potential risks of compromise are great, then perhaps the alternative to computerizing everything is to rethink the problems at hand.

References

Mark Eichin and Jon Rochlis, "With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988," MIT Project Athena report, Cambridge, MA 02139, November 1988.

Steven B. Lipner, "Non-Discretionary Controls for Commercial Applications," Proc. IEEE Symposium on Security and Privacy, April 1982, pp. 2-10.

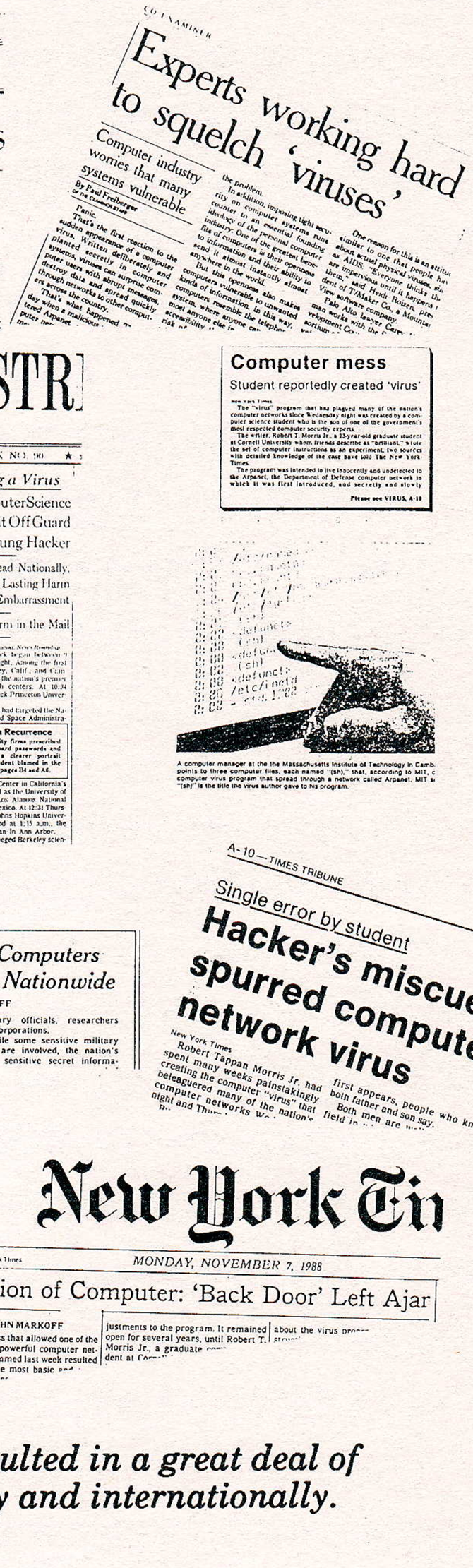
Donn Seeley, "A Tour of the Worm," Proc. USENIX, San Diego CA, February, 1989.

John F. Shoch & Jon A. Hupp, "The Worm Programs—Early Experience with Distributed Computation," Comm. ACM 25 3, March 1982, pp. 172-180.

Eugene H. Spafford, "The Internet Worm Program: An Analysis," ACM SIGCOMM *Computer Communication Review* 19 1, January 1989, pp. 18-57.

Cliff Stoll, "Stalking the Wily Hacker," Comm. of the ACM, 31, 5, May 1988, pp. 484-497.

PETER G. NEUMANN has been a member of the Computer Science Laboratory at SRI International in Menlo Park, California since 1971, where he has worked on systems that satisfy stringent requirements for security, reliability, and safety, and on formal methodology for systems development and verification. At Bell Labs throughout the 1960s, he did research in computers and communications, and played a major role in the Multics development at MIT (1965-69). He has A.B. (1954), S.M. (1955), and Ph.D. (1961) degrees from Harvard and a Dr. rerum naturarum from the Technische Hochschule, Darmstadt, Germany, 1960 (where he was a Fulbright scholar for two years). He has taught at Stanford and Berkeley. He is Chairman of the ACM Committee on Computers and Public Policy, Moderator of the ACM RISKS Forum, and Editor of the ACM SIGSOFT *Software Engineering Notes*.



A computer manager at the the Massachusetts Institute of Technology in Cambpoints to three computer files, each named "(sh)," that, according to MIT, c computer virus program that spread through a network called Arpanet. MIT s "(sh)" is the title the virus author gave to his program.

The Internet Worm incident resulted in a great deal of press coverage both nationally and internationally.

Ethics and the Internet (RFC 1087)

by the Internet Activities Board

Status of this memo

This memo is a statement of policy by the Internet Activities Board (IAB) concerning the proper use of the resources of the Internet. Distribution of this memo is unlimited.

Introduction

At great human and economic cost, resources drawn from the U.S. Government, industry and the academic community have been assembled into a collection of interconnected networks called the *Internet*. Begun as a vehicle for experimental network research in the mid-1970's, the Internet has become an important national infrastructure supporting an increasingly widespread, multi-disciplinary community of researchers ranging, inter alia, from computer scientists and electrical engineers to mathematicians, physicists, medical researchers, chemists, astronomers and space scientists.

As is true of other common infrastructures (e.g., roads, water reservoirs and delivery systems, and the power generation and distribution network), there is widespread dependence on the Internet by its users for the support of day-to-day research activities.

The reliable operation of the Internet and the responsible use of its resources is of common interest and concern for its users, operators and sponsors. Recent events involving the hosts on the Internet and in similar network infrastructures underscore the need to reiterate the professional responsibility every Internet user bears to colleagues and to the sponsors of the system. Many of the Internet resources are provided by the U.S. Government. Abuse of the system thus becomes a Federal matter above and beyond simple professional ethics.

IAB Statement of Policy

The Internet is a national facility whose utility is largely a consequence of its wide availability and accessibility. Irresponsible use of this critical resource poses an enormous threat to its continued availability to the technical community.

The U.S. Government sponsors of this system have a fiduciary responsibility to the public to allocate government resources wisely and effectively. Justification for the support of this system suffers when highly disruptive abuses occur. Access to and use of the Internet is a privilege and should be treated as such by all users of this system.

The IAB strongly endorses the view of the Division Advisory Panel of the National Science Foundation Division of Network, Communications Research and Infrastructure which, in paraphrase, characterized as unethical and unacceptable any activity which purposely:

- seeks to gain unauthorized access to the resources of the Internet
- disrupts the intended use of the Internet
- wastes resources (people/capacity/computer) through such actions
- destroys the integrity of computer-based information, and/or
- compromises the privacy of users.

The Internet exists in the general research milieu. Portions of it continue to be used to support research and experimentation on networking. Because experimentation on the Internet has the potential to affect all of its components and users, researchers have the responsibility to exercise great caution in the conduct of their work. Negligence in the conduct of Internet-wide experiments is both irresponsible and unacceptable.

The IAB plans to take whatever actions it can, in concert with Federal agencies and other interested parties, to identify and to set up technical and procedural mechanisms to make the Internet more resistant to disruption. Such security, however, may be extremely expensive and may be counterproductive if it inhibits the free flow of information which makes the Internet so valuable. In the final analysis, the health and well-being of the Internet is the responsibility of its users who must, uniformly, guard against abuses which disrupt the system and threaten its long-term viability.

A Letter to the Editor

Mr. Jacobsen,

I recently read John Quarterman's article entitled "Mail Through the Matrix" in the February 1989 issue of *ConneXions*, and would like to make a clarification.

When discussing the concept of enveloping, Mr. Quarterman indicates that X.400, the CCITT Recommendation on Message Handling Systems, does not appear to distinguish between the envelope and header of a message. This is *not* the case.

The X.400 recommendations make an absolute distinction between the envelope and header of messages. The separation allows the Message Transfer System (MTS) to relay messages which are entirely opaque. The envelope contains all the required information to complete delivery and any header is contained within the opaque message that is being transferred. This is a significant strong point of X.400, allowing the service to be general enough to not only carry conventional electronic mail, Interpersonal Messages (IPMS) in X.400, but also EDI documents, store-and-forward file transfer, encrypted mail, and so on.

Sincerely,

Christopher W. Moore
Senior Software Engineer
The Wollongong Group, Inc.

While the article in question was not a tutorial on X.400, we do appreciate the clarification. Needless to say, our goal is to present information as accurately as possible, and we apologize for any confusion which may have arisen from this. X.400 will be explained more thoroughly in an upcoming article by Julian Onions of the University of Nottingham. The article is part of our new series called "Components of OSI." —*Ed.*

CONNEXIONS
480 San Antonio Road
Suite 100
Mountain View, CA 94040

FIRST CLASS MAIL
U.S. POSTAGE
PAID
SAN JOSE, CA
PERMIT NO. 1

CONNEXIONS

PUBLISHER Daniel C. Lynch

EDITOR Ole J. Jacobsen